UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/659,834	09/10/2003	Tamio Saito	ESMART-0003	5947

7590 02/16/2006

David B. Ritchie
Thelen Reid & Priest LLP
P.O. Box 640640
San Jose, CA 95164

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 02/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/659,834	SAITO ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-6,9-15 and 17-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3-6,9-15 and 17-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 1-27-06/1-3-06
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 3-6, 9-15, and 17-55 are pending in this actions, claims 29-55 are newly added.

Rejections

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

3. Claims 3-6, 9-13, 18-20, 24, 25, 27-29, 31-34, 36, 37, 40-43, and 47-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shen (E.P. No. 1,074,949) in view of any of [Ritter (U.S. Patent Pub. No. 2002/0111164), McPhillie et al. (UK Patent Application No. GB 2 2336 005 A), and Setlak et al. (U.S. Patent No. 5,852,670)]. The independent claims are very similar, only varying in the details taught by each of the references listed above. Because of this, examiner shows the teachings of each independent claim separately, but groups the dependent claims together.

Regarding claim 3, Shen teaches an intelligent identification card comprising:

- An on-board memory for storing reference data (fig. 1, ref. num 11);
- An on-board sensor for capturing live biometric data (fig. 1, ref. num 12);

- An on-board microprocessor for comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and for generating a verification message only if there is a match within a predetermined threshold (fig. 1, ref. num 14 and col. 3, lines 9-21); and
- **An interface** for communicating the verification message to an external network (fig. 1, ref. num 13),
- Wherein the verification message includes at least excerpts from the stored reference data (col. 3, lines 31-36).

Shen does not teach wherein the verification message includes at least excerpts from the captured biometric data.

Ritter teaches wherein the verification message includes at least excerpts from the captured biometric data (paragraph 0042 and 0072).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine including an excerpt from the captured biometric data in the verification message, as taught by Ritter, with the apparatus of Shen. It would have been obvious for such modifications because the supplied biometric data is used to determine if the identity of the user is verified (see paragraph 0072 of Ritter).

Regarding claim 30, Shen teaches an intelligent identification card comprising:

- An on-board sensor for capturing live biometric data (fig. 1, ref. num 12);
- A first on-board processor coupled with said on-board sensor (fig. 1, ref. num 14), said first on-board processor including a memory storing reference data (fig. 1, ref. num 11), said first on-board processor comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and generating a verification message only if there is a match within a predetermined threshold (col. 3, lines 9-21); and
- An interface coupled to either one of said first on-board processor and said second on-board processor, for communicating with an external network, the verification message being transmitted to the external network via said interface (fig. 1, ref. num 13 and col. 3, lines 31-36).

Shen does not teach a second on-board processor coupled with said first on-board processor, for executing intelligent card functions.

McPhillie et al. teaches a second on-board processor coupled with said first on-board processor, for executing intelligent card functions (fig. 4, ref. num 119).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a second on-board processor for executing intelligent card functions, as taught by McPhillie et al., with the apparatus of Shen. It would have

been obvious for such modifications because utilizing a second co-processor for a specific purpose makes the processor faster.

Regarding claims 38, 52, and 55, Shen teaches an intelligent identification card/method/apparatus for identifying identity of a user of an intelligent identification card, the intelligent identification card including an on-board memory storing reference data and an on-board fingerprint sensor (fig. 1, ref. num 11 and 12), said method comprising:

- An on-board fingerprint sensor for capturing fingerprint data (fig. 1, ref. num 12);
- An indicator for providing real-time feedback (col. 4, lines 18-23);
- An on-board microprocessor for comparing the captured fingerprint data with corresponding stored reference data within a predetermined threshold and for generating a verification message only if there is a match within a predetermined threshold (col. 3, lines 9-21); and
- An interface for communicating the verification message to an external network (fig. 1, ref. num 13 and col. 3, lines 31-36).

Shen does not specifically teach that the indicator is for finger placement purposes.

Setlak et al. teaches the indicator is for finger placement purposes (fig. 25, ref. num 39).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine indicating in real-time if the user is placing their finger correctly in the fingerprint sensor, as taught by Setlak et al., with the apparatus of Shen. It would have been obvious for such modifications because the feedback ensures proper placement of the finger in order to get a good read of the supplied fingerprint data.

Regarding claims 39 and 53, Shen teaches a method/apparatus for identifying a user of an intelligent identification card, the intelligent identification card including an on-board memory storing reference data and an on-board biometric sensor (fig. 1, ref. num 11 and 12), said method/apparatus comprising:

- Capturing live biometric data using the on-board sensor (fig. 1, ref. num 12);
- Comparing the captured biometric data with corresponding reference data stored in the on-board memory within a predetermined threshold (col. 3, lines 9-16);
- Generating a verification message only if there is a match within a predetermined threshold (col. 3, lines 16-21); and
- Communicating the verification message to an external network (fig. 1, ref. num 13),
- Wherein the verification message includes at least excerpts from the stored reference data (col. 3, lines 31-36).

Shen does not teach wherein the verification message includes at least excerpts from the captured biometric data.

Ritter teaches wherein the verification message includes at least excerpts from the captured biometric data (paragraph 0042 and 0072).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine including an excerpt from the captured biometric data in the verification message, as taught by Ritter, with the apparatus of Shen. It would have been obvious for such modifications because the supplied biometric data is used to determine if the identity of the user is verified (see paragraph 0072 of Ritter).

Regarding claims 45 and 54, Shen teaches a method/apparatus for identifying a user of an intelligent identification card, the intelligent identification card including an on-board memory storing reference data (fig. 1, ref. num 11), an on-board biometric sensor (fig. 1, ref. num 12), and an ISO card processor (fig. 1, ref. num 14), said method/apparatus comprising:

- Capturing live biometric data using the on-board sensor (fig. 1, ref. num 12);
- Comparing, the captured biometric data with corresponding reference data stored in the on-board memory within a predetermined threshold (col. 3, lines 9-16);

- Generating, using the security processor, a verification message only if there is a match within a predetermined threshold (col. 3, lines 16-21);
- Communicating the verification message to an external network via an interface (fig. 1, ref. num 13 and col. 3, lines 31-36); and
- Allowing operation of the ISO card processor if the identity of the user is verified (col. 3, lines 20-21).

Shen does not teach using a security processor to perform the comparing.

McPhillie et al. teaches using a security processor to perform the comparing (fig. 4, ref. num 119).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a security processor to perform the comparing, as taught by McPhillie et al., with the apparatus of Shen. It would have been obvious for such modifications because utilizing a second co-processor for a specific purpose makes the processor faster.

Regarding claims 4 and 40, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein the verification message is transmitted to a remote authentication system for additional verification (see col. 3, lines 25-41 of Shen).

Regarding claims 5 and 41, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein the remote authentication system includes remotely stored reference data that is different from the locally stored reference data (see col. 3, lines 28-31 of Shen).

Regarding claims 6 and 42, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein the on-board microprocessor uses a different matching algorithm than that used at the remote authentication system (see col. 4, lines 3-8 of Shen).

Regarding claim 9, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein the card is ISO Smartcard compatible (see col. 1, lines 6-20 of Shen).

Regarding claims 10 and 31, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches **wherein said on-board processor is a security processor for storing and processing the protected biometric data, and wherein said identification card further comprises** an ISO Smartcard processor (see fig. 4, ref. num 119 of McPhillie and col. 1, lines 6-20 of Shen, a smartcard that would be used to replace all other cards would inherently be compatible to the ISO standard).

Regarding claims 11-13, 32-34, 47, and 48, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein **the** security processor is functionally separated from the ISO Smartcard processor by a firewall, all external data to and from the security

processor passes through the ISO Smartcard processor, and all external data to and from the ISO Smartcard processor passes through the security processor (see fig. 3-5 and page 7, line 7 through page 12, line 21 of McPhillie et al.).

Regarding claims 18 and 49, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein the biometric data includes fingerprint data and the sensor is a fingerprint sensor which captures data from a user's finger placed on the sensor (see fig. 1, ref. num 12 of Shen).

Regarding claims 19 and 50, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches **further comprising an indicator providing** real-time feedback **for finger placement** while the user is manipulating his **or her** finger over the fingerprint sensor, thereby facilitating an **adequate** placement of the finger over the sensor (see col. 4, lines 18-23 of Shen and fig. 25, ref. num 39 of Setlak et al.).

Regarding claims 20 and 51, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein the matching process utilizes a hybrid matching algorithm that takes into account both minutiae and overall spatial relationships in the captured biometric data (see col. 3, lines 42-57 of Shen).

Regarding claim 24, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein the card further comprises means for restricting use of the card to a predetermined location (see col. 1, lines 6-14 of Shen).

Regarding claims 25 and 43, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein at least some of the captured biometric data and the reference data are transmitted to a separate authentication server for secure verification of a user's identity prior to any grant of on-line access to an application server for processing of secure financial transactions involving that user (see col. 3, lines 28-36 of Shen).

Regarding claim 27, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein the output from the card is used to obtain physical access into a secure area (see col. 1, lines 9-12 of Shen).

Regarding claim 28, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein a record of successful and unsuccessful access attempts is maintained on the card (see col. 4, lines 8-17 of Shen).

Regarding claim 29, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein said interface includes at least one of an electrical contact interface and a wireless communication interface (see fig. 1, ref. num 13 of Shen).

Regarding claim 36, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches further comprising an on-board location detector for determining current location of the identification card and means for restricting use of the card based on the detected location (see paragraph 0034 of Ritter).

Regarding claim 37, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein said on-board location detector includes a GPS signal receiver (see paragraph 0034 of Ritter).

Claims 14, 15, 35, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shen (E.P. No. 1,074,949) in view of [Ritter/McPhillie et al./Setlak et al.], and further in view of Cassista et al. (U.S. Patent Pub. No. 2002/0007459).

Regarding claims 14, 15, 35, and 46, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches all the limitations of claims 3, 9, 10, & 30, 31, 34, & 45, above. However, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] does not teach the security processor has a first connection used for loading data during a loading process and a second connection connected to an external network and the first connection is permanently disabled after the loading process has been completed.

Cassista et al. teaches the security processor has a first connection used for loading data during a loading process and a second connection connected to an

external network and the first connection is permanently disabled after the loading process has been completed (paragraph 0120).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine two connections on the card, one that is disabled after the initial loading is completed, as taught by Cassista et al., with the card of Shen/[Ritter/McPhillie et al./Setlak et al.] It would have been obvious for such modifications because disabling the connection path helps limit the amount of battery draw from the circuit because there is no need to transmit data across that disabled line (paragraph 0120 of Cassista et al.).

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shen (E.P. No. 1,074,949) in view of [Ritter/McPhillie et al./Setlak et al.], and further in view of Powell (U.S. Patent No. 6,456,980).

Regarding claim 17, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches wherein the biometric sensor is a fingerprint sensor (see col. 3, lines 9-12 of Shen); and the security processor, the ISO Smartcard processor and the fingerprint sensor are all located in a middle region between the upper region and the lower region (see fig. 1 of Shen).

Shen as modified by [Ritter/McPhillie et al./Setlak et al.] does not specifically teach the card comprises an upper magnetic stripe region and a lower embossed region.

Powell teaches the card comprises an upper magnetic stripe region and a lower embossed region (fig. 5A and 5B and col. 4, line 61 through col. 5, line 5).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine an upper magnetic region and a lower embossed region, as taught by Powell, with the card of Shen/[Ritter/McPhillie et al./Setlak et al.] It would have been obvious for such modifications because the upper magnetic region allows for conventional credit card readers to read the card and the lower embossed region allows the users name to be displayed (see col. 5, lines 1-5 of Powell).

Claims 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shen (E.P. No. 1,074,949) in view of [Ritter/McPhillie et al./Setlak et al.], and further in view of Neuhaus et al. (U.S. Patent No. 6,853,087).

Regarding claims 21-23, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches all the limitations of claims 3 and 18, above. However, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] does not teach wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate, the backing plate

comprises a glass epoxy layer sandwiched between two metal layers, and the backing plate is reinforced by a carrier frame surrounding the sheet of silicon.

Neuhaus et al. teaches wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate, the backing plate comprises a glass epoxy layer sandwiched between two metal layers, and the backing plate is reinforced by a carrier frame surrounding the sheet of silicon (col. 4, line 62 through col. 5, line 17).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a silicon fingerprint sensor, epoxy backing, and reinforcing the backing by a carrier frame, as taught by Neuhaus et al., with the card of Shen/[Ritter/McPhillie et al./Setlak et al.] It would have been obvious for such modifications because the materials used provide protection of the chip.

Claims 26 and 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shen (E.P. No. 1,074,949) in view of [Ritter/McPhillie et al./Setlak et al.], and further in view of Krajewski et al. (U.S. Patent No. 5,590,199).

Regarding claims 26 and 44, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] teaches all the limitations of claims 3, 25 & 39, above. However, Shen as modified by [Ritter/McPhillie et al./Setlak et al.] does not teach wherein in response to a match request relating to a particular logon attempt at a particular application server which

produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card as, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid.

Krajewski et al. teaches wherein in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card as, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid (col. 6, line 37 through col. 7, line 23).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed which

verifies whether the challenge response is valid, as taught by Krajewski et al., with the card of Shen/[Ritter/McPhillie et al./Setlak et al.] It would have been obvious for such modifications because challenge/response systems allow devices to verify a secret without having to exchange the secret in the clear. It would be useful to do this because the devices can ensure security without having to establish a common secret beforehand.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100